

(2) Department Order 2620.6 entitled, “Procedures for Requesting a Department of Justice Security Clearance for Non-Contractor Personnel Outside the Executive Branch.”

(3) Department Order 2600.3A entitled, “Requirements for Safeguarding Classified Information and Material Released to Industry in Connection with Contracts or Grants.”

(4) Department Order 2660.1A entitled, “Department of Justice Special Security Center (Room 6744—Main Justice).”

(5) Offices, Boards and Divisions (OBD) Order 2710.3A entitled, “Files Maintenance and Records Disposition.”

§ 17.3 Applicability.

This regulation governs the Department’s National Security Information Program and takes precedence over all Department publications affecting that program. It establishes, for uniform application throughout the Department, the policies, standards, criteria and procedures for the classification, downgrading, declassification and safeguarding of National Security Information originated, produced or handled by, or in the custody of, the Department.

§ 17.4 Application to non-Executive Branch personnel.

Except as otherwise provided herein (see § 17.96), the provisions of this regulation apply to non-contractor personnel outside of the Executive Branch and to contractor personnel or employees who are entrusted with National Security Information originated within or in the custody of the Department. Clearance procedures for the aforementioned personnel are contained in Department Orders 2620.6 and 2600.3A, respectively. Procedures for clearing Department personnel are contained in § 17.98 of this regulation.

§ 17.5 Atomic Energy Act.

Nothing in this regulation supersedes any requirements made by or under the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011–2394. “Restricted Data” shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amend-

ed, 42 U.S.C. 2161–2166, and the regulations issued pursuant thereto.

Subpart B—Security Classification

§ 17.6 Policy.

(a) Except as provided in § 17.5, Executive Order 12356, as implemented by this regulation, provides the only basis for classifying information.

(b) Unnecessary classification and higher than necessary classification shall be scrupulously avoided.

(c) Classification shall be continued no longer than is necessary for the protection of national security.

(d) Information may not be classified except for the purposes of preventing damage to the national security.

§ 17.7 Classification levels.

(a) *General.* Official information which requires protection against unauthorized disclosure in the interests of national security shall be classified in one of three levels, namely, “Top Secret,” “Secret” or “Confidential.” No other terms shall be used to identify official information as requiring protection in the interests of national security, except as otherwise expressly provided by statute.

(b) *Top Secret.* “Top Secret” is the designation which shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of “exceptionally grave damage” could include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of extremely sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with restraint.

(c) *Secret.* “Secret” is the designation which shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of “serious damage”